

DIN EN 62304
(VDE 0750-101)
DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.

VDE

ICS 35.240.80

Ersatz für

DIN EN 62304**(VDE 0750-101):2007-03** und**DIN EN 62304 Berichtigung 1****(VDE 0750-101 Berichtigung 1):2009-05**

Siehe Anwendungsbeginn

Medizingeräte-Software –
Software-Lebenszyklus-Prozesse
(IEC 62304:2006 + A1:2015);
Deutsche Fassung EN 62304:2006 + Cor.:2008 + A1:2015

Medical device software –

Software life-cycle processes

(IEC 62304:2006 + A1:2015);

German version EN 62304:2006 + Cor.:2008 + A1:2015

Logiciels de dispositifs médicaux –

Processus du cycle de vie du logiciel

(IEC 62304:2006 + A1:2015);

Version allemande EN 62304:2006 + Cor.:2008 + A1:2015

Gesamtumfang 101 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
 DIN-Normenausschuss Rettungsdienst und Krankenhaus (NARK)
 DIN-Normenausschuss Medizin (NAMed)

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2006-06-01 angenommene Europäische Norm und die am 2015-07-31 angenommene Änderung A1 als DIN-Norm ist 2016-10-01.

Für **DIN EN 62304 (VDE 0750-101):2007-03** und **DIN EN 62304 Berichtigung 1 (VDE 0750-101 Berichtigung 1):2009-05** besteht eine Übergangsfrist bis 2018-07-31.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62304 (VDE 0750-101):2013-10.

Für dieses Dokument ist das nationale Arbeitsgremium UK 811.3 „Sicherheit von medizinisch genutzten Geräten/Systemen/Einrichtungen in der vernetzten Anwendung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 62A „Common aspects of electrical equipment used in medical practice“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

In dieser Norm sind die eingearbeiteten Änderungen der Änderung 1 mit einem senkrechten Strich am linken Rand des Textes markiert.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber **DIN EN 62304 (VDE 0750-101):2007-03** und **DIN EN 62304 Berichtigung 1 (VDE 0750-101 Berichtigung 1):2009-05** wurden folgende Änderungen vorgenommen:

- a) Erweiterung des Anwendungsbereichs auf Legacy-Software;
- b) Einführung von Begriffen aus DIN EN 14971;
- c) Optimierung der Prozessbeschreibung;
- d) Anpassung von Tabelle C.3 an DIN EN 60601-1 (VDE 0750-1):2013-12;
- e) die Deutsche Fassung wurde in den Abschnitten 2 und 3 sowie den Anhängen ZA und ZZ an die aktuellen Standardtexte angepasst.

Frühere Ausgaben

DIN EN 62304 (VDE 0750-101): 2007-03
DIN EN 62304 Berichtigung 1 (VDE 0750-101 Berichtigung 1): 2009-05

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Dokumenten

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden Deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 60601-1:2006 + Cor.:2010 + A1:2013	IEC 60601-1:2005 + Cor.:2006 + Cor.:2007 + A1:2012	DIN EN 60601-1 (VDE 0750-1):2007-07 <i>ersetzt durch:</i> DIN EN 60601-1 (VDE 0750-1):2013-12	VDE 0750-1 VDE 0750-1
EN 60601-1-4	IEC 60601-1-4	DIN EN 60601-1-4 (VDE 0750-1-4)	VDE 0750-1-4
EN 60601-1-6	IEC 60601-1-6	DIN EN 60601-1-6 (VDE 0750-1-6)	VDE 0750-1-6
EN 61010-1:2010	IEC 61010-1:2010	DIN EN 61010-1 (VDE 0411-1):2011-07	VDE 0411-1
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803
–	IEC 62366-1	–	–
–	IEC 80001-1:2010	–	–
–	IEC/TR 80002-1:2009	–	–
–	IEC/DIS 82304-1	–	–
–	ISO 9000:2000 <i>ersetzt durch:</i> ISO 9000:2015	–	–
–	ISO 9001:2008 <i>ersetzt durch:</i> ISO 9001:2015	–	–
EN ISO 14121-1 <i>ersetzt durch:</i> EN ISO 12100	ISO 14121-1 <i>ersetzt durch:</i> ISO 12100	DIN EN ISO 14121-1 <i>ersetzt durch:</i> DIN EN ISO 12100	– –

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
–	ISO/IEC 14764:1999 <i>ersetzt durch:</i>	–	–
–	ISO/IEC 14764:2006	–	–
–	ISO/IEC 15504-5:2012	–	–
–	ISO/IEC 16085	–	–
–	ISO/IEC 25010:2011	–	–
–	ISO/IEC 33001	–	–
–	ISO/IEC 33004	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 60601-1 (VDE 0750-1):2013-12, Medizinische elektrische Geräte – Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale (IEC 60601-1:2005 + Cor.:2006 + Cor.:2007 + A1:2012); Deutsche Fassung EN 60601-1:2006 + Cor.:2010 + A1:2013

DIN EN 60601-1-4 (VDE 0750-1-4), Medizinische elektrische Geräte – Teil 1-4: Allgemeine Festlegungen für die Sicherheit – Ergänzungsnorm: Programmierbare elektrische medizinische Systeme

DIN EN 60601-1-6 (VDE 0750-1-6), Medizinische elektrische Geräte – Teil 1-6: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale – Ergänzungsnorm: Gebrauchstauglichkeit

DIN EN 61010-1 (VDE 0411-1):2011-07, Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte – Teil 1: Allgemeine Anforderungen (IEC 61010-1:2010); Deutsche Fassung EN 61010-1:2010

DIN EN 61508-5 (VDE 0803) (alle Teile), Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme

DIN EN ISO 12100, Sicherheit von Maschinen – Allgemeine Gestaltungsgrundsätze – Risikobeurteilung und Risikominderung

Deutsche Fassung

**Medizingeräte-Software –
Software-Lebenszyklus-Prozesse**
(IEC 62304:2006 + A1:2015)

Medical device software –
Software life-cycle processes
(IEC 62304:2006 + A1:2015)

Logiciels de dispositifs médicaux –
Processus du cycle de vie du logiciel
(IEC 62304:2006 + A1:2015)

Diese Europäische Norm wurde von CENELEC am 2006-06-01 und die A1 am 2015-07-31 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

© 2015 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 62304:2006 + A1:2015 D



Documents

Document Sharing Hub

Vorwort

Der Text des Schriftstücks 62A/523/FDIS, zukünftige 1. Ausgabe von IEC 62304, wurde von einer gemeinsamen Arbeitsgruppe zwischen SC 62A „Überarbeitung und Anpassung der allgemeinen Bestimmungen“ des Technischen Komitees TC 62 „Allgemeine Bestimmungen für elektrische Einrichtungen in medizinischer Anwendung“ und dem Technischen Komitee ISO/TC 210 „Qualitätsmanagement und allgemeine Aspekte für Medizinprodukte“ ausgearbeitet. Dieser Text wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2006-06-01 als EN 62304 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2007-03-01
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2009-06-01

In dieser Norm werden die folgenden Schriftarten verwendet:

- Festlegungen und Definitionen: Normalschrift;
- Informationen außerhalb von Tabellen, wie z. B. Anmerkungen und Referenzen, in Kleinschrift. Normativer Text von Tabellen: Kleinschrift;
- IN DIESER NORM BENUTZTE BEGRIFFE, DIE IN ABSCHNITT 3 DEFINIERT SIND UND IM VERZEICHNIS DER DEFINIERTEN BEGRIFFE ANGEZEIGT SIND: KAPITÄLCHEN.

Ein Stern (*) am ersten Zeichen einer Überschrift oder am Anfang eines Abschnittes bedeutet, dass erklärende Hinweise im [Anhang B](#) gegeben werden.

Tabelle C.5 wurde vom ISO/IEC JTC 1/SC 7 „Software und System-Engineering“ erstellt.

Diese Europäische Norm wurde unter einem an CENELEC von der Europäischen Kommission und der Europäischen Freihandelszone erteilten Mandat ausgearbeitet und unterstützt die grundsätzlichen Anforderungen der EG-Richtlinien 93/42/EWG, 90/385/EG und 98/79/EG. Siehe Anhang ZZ.

Die Anhänge ZA und ZZ wurden von CENELEC hinzugefügt.

Der Inhalt des in 2008-11 veröffentlichten Corrigendums ist in dieser Fassung enthalten.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62304:2006 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60601-1-4 + A1	ANMERKUNG	Harmonisiert als EN 60601-1-4:1996 + A1:1999 (nicht modifiziert).
IEC 61508-3	ANMERKUNG	Harmonisiert als EN 61508-3:2001 (nicht modifiziert).
IEC 61010-1	ANMERKUNG	Harmonisiert als EN 61010-1:2001 (nicht modifiziert).
ISO 9000	ANMERKUNG	Harmonisiert als EN ISO 9000:2005 (nicht modifiziert).

ISO 9001	ANMERKUNG	Harmonisiert als EN ISO 9001:2000 (nicht modifiziert).
ISO 13485	ANMERKUNG	Harmonisiert als EN ISO 13485:2003 (nicht modifiziert).
IEC 60601-1-6	ANMERKUNG	Harmonisiert als EN 60601-1-6:2004 (nicht modifiziert).

Europäisches Vorwort zu A1

Der Text des Dokuments 62A/1007/FDIS, zukünftige IEC 62304:2006/A1, erarbeitet vom SC 62A „Common aspects of electrical equipment used in medical practice“ des IEC/TC 62 „Electrical equipment in medical practice“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 62304:2006/A1:2015 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2016-05-01
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2018-07-31

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde, und unterstützt grundlegende Anforderungen der EU-Richtlinie.

Zum Zusammenhang mit EU-Richtlinie 93/42/EEC, 98/79/EC, 90/385/EEC, siehe den informativen Anhang ZZ, der Bestandteil der EN 62304:2006/corrigendum Nov. 2008 ist.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62304:2006/A1:2015 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

Ersetze die bestehenden Verweisungen mit den folgenden:

IEC 60601-1:2005	ANMERKUNG	Harmonisiert als EN 60601-1:2006.
IEC 60601-1:2005/AMD1:2012	ANMERKUNG	Harmonisiert als EN 60601-1:2006/A1:2013.
IEC 60601-1-4:1996	ANMERKUNG	Harmonisiert als EN 60601-1-4:1996.

IEC 60601-1-4:1996/AMD1:1999	ANMERKUNG	Harmonisiert als EN 60601-1-4:1996/A1:1999.
IEC 60601-1-6	ANMERKUNG	Harmonisiert als EN 60601-1-6.
IEC 61508-3	ANMERKUNG	Harmonisiert als EN 61508-3.
IEC 61010-1:2010	ANMERKUNG	Harmonisiert als EN 61010-1:2010.
ISO 9000:2005	ANMERKUNG	Harmonisiert als EN ISO 9000:2005.
ISO 9001:2008	ANMERKUNG	Harmonisiert als EN ISO 9001:2008.
ISO 13485:2003	ANMERKUNG	Harmonisiert als EN ISO 13485:2003.
IEC 62366-1:2015	ANMERKUNG	Harmonisiert als EN 62366-1:2015.
IEC 82304-1	ANMERKUNG	Harmonisiert als EN 82304-1 ⁴⁾ .

⁴⁾ Im Entwurfsstadium.

Inhalt

	Seite
Vorwort	2
Europäisches Vorwort zu A1	3
Einleitung	10
1 Anwendungsbereich	14
1.1 *Zweck	14
1.2 *Anwendungsgebiet	14
1.3 Beziehung zu anderen Normen	14
1.4 Einhaltung	14
2 *Normative Verweisungen	15
3 *Begriffe	15
4 *Allgemeine Anforderungen	21
4.1 *Qualitätsmanagement-System	21
4.2 *RISIKOMANAGEMENT	22
4.3 *Software-Sicherheitsklassifizierung	22
4.4 *ÄLTERE SOFTWARE	23
4.4.1 Allgemeines	23
4.4.2 RISIKOMANAGEMENT-AKTIVITÄTEN	24
4.4.3 Lückenanalyse	24
4.4.4 Aktivitäten für das Schließen der Lücken	24
4.4.5 Begründung für die Benutzung der ÄLTEREN SOFTWARE	25
5 Software-Entwicklungs-PROZESS	25
5.1 *Planung der Software-Entwicklung	25
5.1.1 Software-Entwicklungsplan	25
5.1.2 Aktualisierung des Software-Entwicklungsplans	25
5.1.3 Referenz im Software-Entwicklungsplan auf SYSTEM-Design und -Entwicklung	25
5.1.4 Planung von Normen, Methoden und Werkzeugen der Software-Entwicklung	26
5.1.5 Planung der Software-Integration und der Integrationsprüfung	26
5.1.6 Planung der Software-VERIFIZIERUNG	26
5.1.7 Planung des Software-RISIKOMANAGEMENTS	26
5.1.8 Planung der Dokumentation	26
5.1.9 Planung des Software-Konfigurationsmanagements	27
5.1.10 Zu kontrollierende unterstützende Komponenten	27
5.1.11 Kontrolle der Software-KONFIGURATIONSELEMENTE vor der VERIFIZIERUNG	27
5.1.12 Identifizierung und Vermeidung gemeinsamer Software-Fehler	27
5.2 *Analyse der Software-Anforderungen	28
5.2.1 Ableitung der Software-Anforderungen aus den SYSTEM-Anforderungen und Dokumentation	28
5.2.2 Inhalt der Software-Anforderungen	28

	Seite
5.2.3 Einbeziehen von RISIKOBEHERRSCHUNGS-Maßnahmen in die Software-Anforderungen	29
5.2.4 Erneute EVALUATION der RISIKOANALYSE	29
5.2.5 Aktualisierung von Anforderungen	29
5.2.6 VERIFIZIERUNG von Software-Anforderungen	29
5.3 *Design der Software-ARCHITEKTUR	30
5.3.1 Umsetzung von Software-Anforderungen in eine ARCHITEKTUR	30
5.3.2 Entwicklung einer ARCHITEKTUR für die Schnittstellen zwischen SOFTWARE-KOMPONENTEN.....	30
5.3.3 Spezifikation der Funktions- und Leistungsanforderungen für SOUP-Komponenten	30
5.3.4 Spezifikation der für die SOUP-Komponente erforderliche SYSTEM-Hardware und -Software	30
5.3.5 Festlegung der für die RISIKOBEHERRSCHUNG erforderlichen Abgrenzung	30
5.3.6 VERIFIZIERUNG der Software-ARCHITEKTUR	30
5.4 *Detailliertes Software-Design.....	31
5.4.1 Aufteilung der Software in SOFTWARE-EINHEITEN	31
5.4.2 Entwicklung eines detaillierten Designs für jede SOFTWARE-EINHEIT	31
5.4.3 Entwicklung eines detaillierten Designs für Schnittstellen	31
5.4.4 VERIFIZIERUNG des detaillierten Designs	31
5.5 *Implementierung der SOFTWARE-EINHEITEN	31
5.5.1 Implementierung jeder SOFTWARE-EINHEIT.....	31
5.5.2 Festlegung eines VERIFIZIERUNGSPROZESSES für SOFTWARE-EINHEITEN	31
5.5.3 Akzeptanzkriterien für SOFTWARE-EINHEITEN.....	32
5.5.4 Zusätzliche Akzeptanzkriterien für SOFTWARE-EINHEITEN	32
5.5.5 VERIFIZIERUNG der SOFTWARE-EINHEITEN	32
5.6 *Software-Integration und -Integrationsprüfung	32
5.6.1 Integration der SOFTWARE-EINHEITEN	32
5.6.2 VERIFIZIERUNG der Software-Integration	32
5.6.3 Prüfung der integrierten Software	33
5.6.4 Inhalt der Software-Integrationsprüfung.....	33
5.6.5 EVALUIERUNG der Software-Integrationsprüfverfahren	33
5.6.6 Durchführung von REGRESSIONSPRÜFUNGEN	33
5.6.7 Inhalt von Aufzeichnungen über die Integrationsprüfung.....	33
5.6.8 Verwendung eines Problemlösungs-PROZESSES für Software.....	33
5.7 *Prüfung des SOFTWARE-SYSTEMS	34
5.7.1 Festlegung von Prüfungen für Software-Anforderungen	34
5.7.2 Verwendung eines Problemlösungs-PROZESSES für Software.....	34
5.7.3 Prüfungswiederholung nach Änderungen	34
5.7.4 EVALUIERUNG der SOFTWARE-SYSTEM-Prüfungen.....	34
5.7.5 Inhalte der Aufzeichnungen der SOFTWARE-SYSTEM-Prüfungen.....	34
5.8 *Software-FREIGABE für die Benutzung auf einem SYSTEM-Niveau.....	35
5.8.1 Sicherstellen, dass die VERIFIZIERUNG der Software vollständig ist	35

5.8.2	Dokumentation bekannter restlicher ANOMALIEN	35
5.8.3	Bewertung bekannter restlicher ANOMALIEN	35
5.8.4	Dokumentation freigegebener VERSIONEN	35
5.8.5	Dokumentation, wie freigegebene Software erzeugt wurde	35
5.8.6	Sicherstellen, dass AKTIVITÄTEN und AUFGABEN abgeschlossen sind	35
5.8.7	Archivierung der Software	35
5.8.8	Sicherstellen der zuverlässigen Auslieferung der freigegebenen Software	36
6	Software-Wartungs-PROZESS	36
6.1	*Festlegung eines Plans für die Software-Wartung	36
6.2	*Analyse von Problemen und Änderungen	37
6.2.1	Dokumentation und EVALUATION von Rückmeldungen	37
6.2.1.1	Überwachung von Rückmeldungen	37
6.2.1.2	Dokumentation und EVALUATION von Rückmeldungen	37
6.2.1.3	EVALUATION von PROBLEMBERICHTEN auf Auswirkungen auf die SICHERHEIT	37
6.2.2	Verwendung des Problemlösungs-PROZESSES für Software	37
6.2.3	Analyse der ÄNDERUNGSANFORDERUNGEN	37
6.2.4	Genehmigung von ÄNDERUNGSANFORDERUNGEN	37
6.2.5	Kommunikation mit Anwendern und zuständigen Behörden	37
6.3	*Implementierung von Änderungen	38
6.3.1	Verwendung eines festgelegten PROZESSES für die Implementierung von Änderungen	38
6.3.2	Erneute FREIGABE eines geänderten SOFTWARE-SYSTEMS	38
7	*Software-RISIKOMANAGEMENT-PROZESS	38
7.1	*Analyse von Software, die zu GEFÄHRDUNGSSITUATIONEN beiträgt	38
7.1.1	Identifikation von SOFTWARE-KOMPONENTEN, die zu einer GEFÄHRDUNGSSITUATION beitrugen könnten	38
7.1.2	Identifikation von möglichen Ursachen für den Beitrag zu einer GEFÄHRDUNGSSITUATION	38
7.1.3	EVALUATION veröffentlichter Listen mit ANOMALIEN der SOUP	38
7.1.4	Dokumentation möglicher Ursachen	39
7.2	RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.2.1	Definition von RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.2.2	RISIKOBEHERRSCHUNGS-Maßnahmen, die in Software implementiert werden	39
7.3	VERIFIZIERUNG von RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.3.1	VERIFIZIERUNG von RISIKOBEHERRSCHUNGS-Maßnahmen	39
7.3.2	nicht benutzt	39
7.3.3	Dokumentation der RÜCKVERFOLGBARKEIT	39
7.4	RISIKOMANAGEMENT von Software-Änderungen	40
7.4.1	Analyse von Änderungen an MEDIZINPRODUKTE-SOFTWARE im Hinblick auf die SICHERHEIT	40
7.4.2	Analyse der Auswirkung von Software-Änderungen auf bestehende RISIKOBEHERRSCHUNGS-Maßnahmen	40

	Seite
7.4.3 Durchführung von RISIKOMANAGEMENT-AKTIVITÄTEN basierend auf Analysen.....	40
8 *Software-Konfigurationsmanagement-PROZESS	40
8.1 *Identifizierung der Konfiguration	40
8.1.1 Festlegung von Mitteln zur Identifizierung von KONFIGURATIONSELEMENTEN.....	40
8.1.2 Identifizierung von SOUP	40
8.1.3 Identifizierung der Dokumentation der SYSTEM-Konfiguration	41
8.2 *Änderungskontrolle	41
8.2.1 Genehmigung von ÄNDERUNGSANFORDERUNGEN	41
8.2.2 Implementierung von Änderungen	41
8.2.3 VERIFIZIERUNG von Änderungen	41
8.2.4 Bereitstellung von Mitteln für die RÜCKVERFOLGBARKEIT von Änderungen.....	41
8.3 *Aufzeichnungen über den Status der Konfiguration	41
9 *Problemlösungs-PROZESS für Software	42
9.1 Erstellen von PROBLEMBERICHTEN	42
9.2 Untersuchung des Problems	42
9.3 Unterrichtung beteiligter Stellen	42
9.4 Anwendung des Änderungskontroll-PROZESSES	42
9.5 Aufbewahrung von Aufzeichnungen.....	42
9.6 Analyse von Problemen hinsichtlich Trends.....	42
9.7 VERIFIZIERUNG der Lösung von Software-Problemen	43
9.8 Inhalt von Prüfungsdokumentation.....	43
Anhang A (informativ) Begründung für die Anforderungen dieser Norm.....	44
Anhang B (informativ) Anleitung für die Bestimmungen dieser Norm	47
Anhang C (informativ) Beziehung zu anderen Normen.....	65
Anhang D (informativ) Implementierung	88
Literaturhinweise.....	90
Stichwortverzeichnis der definierten Begriffe deutsch – englisch	92
Stichwortverzeichnis der definierten Begriffe englisch – deutsch	94
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	96
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien.....	97
Bilder	
Bild 1 – Überblick über Software-Entwicklungs-PROZESSE und -AKTIVITÄTEN	11
Bild 2 – Überblick über Software-Wartungs-PROZESSE und -AKTIVITÄTEN.....	12
Bild 3 – Zuordnen einer Software-Sicherheitsklasse.....	22
Bild B.2 – Bildliche Darstellung der Beziehung zwischen GEFÄHRDUNG, Folge von Ereignissen, GEFÄHRDUNGSSITUATION und SCHADEN (ISO 14971:2007, Anhang E)	51
Bild B.1 – Beispiel einer Aufteilung von SOFTWARE-KOMPONENTEN.....	53
Bild C.1 – Beziehung von wichtigen MEDIZINPRODUKTE-Normen zur IEC 62304	66

	Seite
Bild C.2 – Software als Teil des V-Modells	70
Bild C.3 – Anwendung von IEC 62304 mit IEC 61010-1	79
Tabellen	
Tabelle A.1 – Zusammenfassung der Anforderungen nach Software-Sicherheitsklassen	46
Tabelle B.1 – Entwicklungs-(Modell-)Strategien wie in ISO/IEC 12207 definiert	48
Tabelle C.1 – Beziehung zu ISO 13485:2003	67
Tabelle C.2 – Beziehung zu ISO 14971:2007	68
Tabelle C.3 – Beziehung zur IEC 60601-1	72
Tabelle C.5 – Beziehung zu ISO/IEC 12207:2008	81
Tabelle D.1 – Checkliste für kleine Unternehmen ohne zertifiziertes QM-SYSTEM	89

Einleitung

Software ist oft ein integraler Bestandteil der MEDIZINPRODUKTE-Technik. Um die SICHERHEIT und Wirksamkeit eines MEDIZINPRODUKTS, das Software enthält, herzustellen, bedarf es der Kenntnis darüber, was die Software bewirken soll, und des Nachweises darüber, dass die Software diese Wirkung erzielt, ohne unvermeidbare RISIKEN zu verursachen.

Diese Norm stellt einen Rahmen von Lebenszyklus-PROZESSEN mit AKTIVITÄTEN und AUFGABEN bereit, der für den sicheren Entwurf und eine sichere Wartung von MEDIZINPRODUKTE-SOFTWARE erforderlich ist. Diese Norm stellt Anforderungen für jeden Lebenszyklus-PROZESS bereit. Jeder Lebenszyklus-PROZESS besteht aus einem Satz von AKTIVITÄTEN, wobei die meisten AKTIVITÄTEN aus einem Satz von AUFGABEN bestehen.

Als Voraussetzung wird angenommen, dass MEDIZINPRODUKTE-SOFTWARE innerhalb eines Qualitätsmanagement-SYSTEMS (siehe 4.1) und eines RISIKOMANAGEMENT-Systems (siehe 4.2) entwickelt und gewartet wird. Der RISIKOMANAGEMENT-PROZESS ist bereits sehr gut durch die Internationale Norm ISO 14971 abgedeckt. Diesen Vorteil nutzt die IEC 62304, indem sie einen normativen Verweis auf ISO 14971 verwendet. Einige zusätzliche RISIKOMANAGEMENT-Anforderungen werden für Software benötigt, insbesondere, wenn es darum geht, Software-Faktoren zu identifizieren, die zu GEFÄHRDUNGEN beitragen können. Diese Anforderungen werden zusammengefasst und in Abschnitt 7 als Software-RISIKOMANAGEMENT-PROZESS festgehalten.

Ob Software ein Faktor ist, der zu einer GEFÄHRDUNGSSITUATION beiträgt, wird durch die AKTIVITÄT der GEFÄHRDUNGS-Identifikation innerhalb des RISIKOMANAGEMENT-PROZESSES ermittelt. GEFÄHRDUNGSSITUATIONEN, die indirekt durch Software verursacht werden könnten (zum Beispiel durch Bereitstellung irreführender Informationen, die die Anwendung einer unangemessenen Behandlung verursachen könnte), müssen betrachtet werden, wenn ermittelt wird, ob die Software einen maßgeblichen Einfluss hat. Die Entscheidung, Software zur RISIKOBEHERRSCHUNG einzusetzen, wird während der AKTIVITÄT der RISIKOBEHERRSCHUNG innerhalb des RISIKOMANAGEMENT-PROZESSES getroffen. Der von dieser Norm geforderte Software-RISIKOMANAGEMENT-PROZESS muss in den Geräte-RISIKOMANAGEMENT-PROZESS nach ISO 14971 eingebunden sein.

Der Software-Entwicklungs-PROZESS besteht aus einer Anzahl von AKTIVITÄTEN. Diese AKTIVITÄTEN sind in Bild 1 dargestellt und in Abschnitt 5 beschrieben. Weil viele Vorkommnisse im Feld mit dem Service oder der Wartung von medizinischen SYSTEMEN im Zusammenhang stehen, einschließlich unsachgemäßer Software-Updates und Software-Upgrades, wird der Software-Wartungs-PROZESS als ebenso wichtig erachtet wie der Software-Entwicklungs-PROZESS. Der Software-Wartungs-PROZESS ist dem Software-Entwicklungs-PROZESS sehr ähnlich. Er ist in Bild 2 dargestellt und in Abschnitt 6 beschrieben.

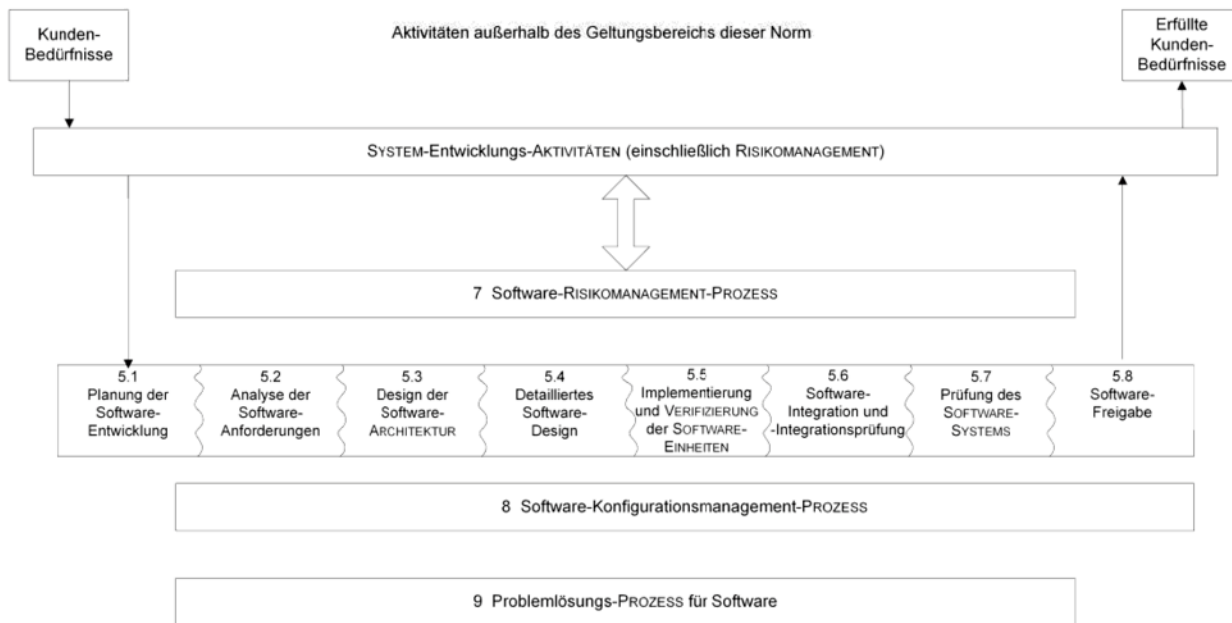


Bild 1 – Überblick über Software-Entwicklungs-PROZESSE und -AKTIVITÄTEN

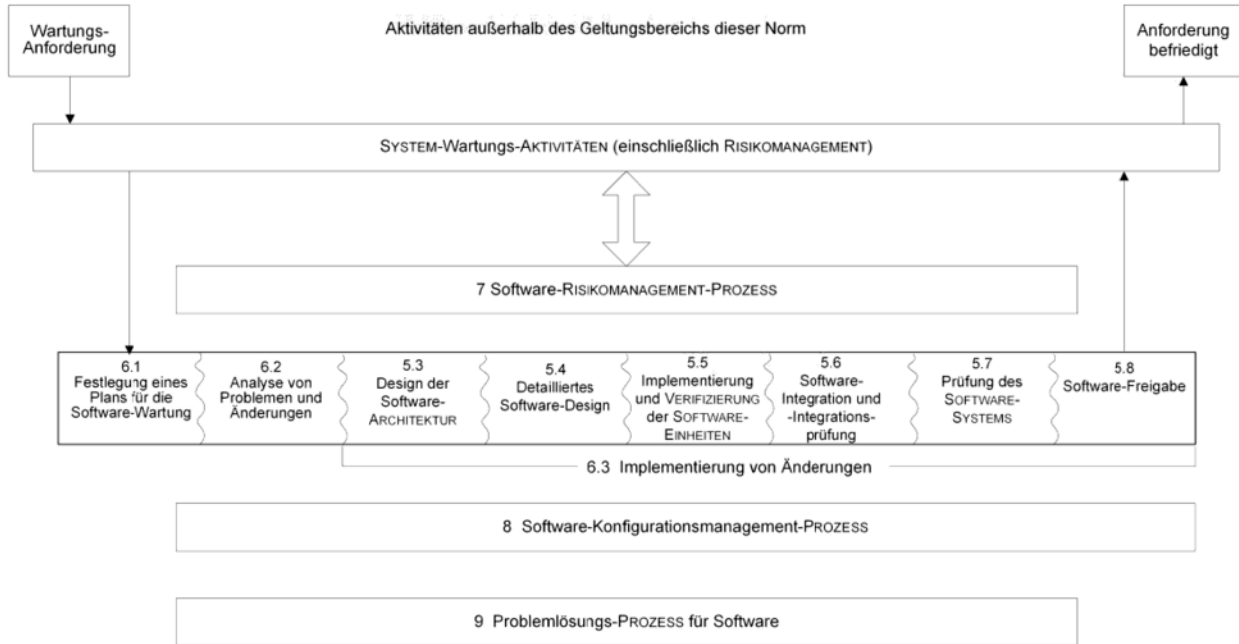


Bild 2 – Überblick über Software-Wartungs-PROZESSE und -AKTIVITÄTEN

Diese Norm identifiziert zwei zusätzliche PROZESSE, die für die Entwicklung von sicherer MEDIZINPRODUKTE-SOFTWARE als wesentlich betrachtet werden. Dies sind der Software-Konfigurations-Management-PROZESS ([Abschnitt 8](#)) und der Problemlösungs-PROZESS für Software ([Abschnitt 9](#)).

Änderung 1 aktualisiert die Norm durch Hinzufügen von Anforderungen bezüglich ÄLTERER SOFTWARE, bei der der Software-Entwicklungsprozess vor dem Vorhandensein der jetzigen Version lag, um Hersteller zu unterstützen, die die Einhaltung der Norm zeigen müssen, um europäische Direktiven zu erfüllen. Änderungen der Software-Sicherheitsklassifizierung enthalten eine Klarstellung von Anforderungen und eine Aktualisierung der Software-Sicherheitsklassifizierung durch Einschluss eines RISIKO-basierten Ansatzes.

Diese Norm schreibt dem HERSTELLER keine Organisationsstruktur vor oder welcher Teil der Organisation welchen PROZESS, welche AKTIVITÄT oder welche AUFGABE durchführen soll. Diese Norm fordert nur, dass der PROZESS, die AKTIVITÄT oder die AUFGABE durchgeführt wird, um die Einhaltung dieser Norm nachzuweisen.

Diese Norm macht keine Vorgaben für die Bezeichnung, das Format oder den expliziten Inhalt der Dokumentation, die zu erstellen ist. Diese Norm erfordert eine Dokumentation der AUFGABEN, aber die Entscheidung, wie diese Dokumentation gestaltet wird, wird dem Benutzer der Norm überlassen.

Diese Norm schreibt kein spezifisches Lebenszyklus-Modell vor. Die Anwender dieser Norm sind verantwortlich für die Auswahl eines Lebenszyklus-Modells für das Software-Projekt und für das Abbilden der PROZESSE, AKTIVITÄTEN und AUFGABEN dieser Norm auf dieses Modell.

[Anhang A](#) enthält die Begründung für die Abschnitte dieser Norm, [Anhang B](#) eine Anleitung für die Umsetzung dieser Norm.

Für diese Norm gilt:

- „muss“ bedeutet, dass die Erfüllung einer Anforderung zwingend ist für die Einhaltung dieser Norm;
- „soll“ bedeutet, dass die Erfüllung einer Anforderung empfohlen wird, aber nicht zwingend ist für die Einhaltung dieser Norm;
- „kann“ wird benutzt, um einen möglichen Weg zu beschreiben, wie die Erfüllung einer Anforderung zu erreichen ist;
- „festlegen“ bedeutet: definieren, dokumentieren und implementieren.
- Wenn diese Norm den Begriff „soweit angemessen“ im Zusammenhang mit einem erforderlichen PROZESS, einer AKTIVITÄT, einer AUFGABE oder einem Ergebnis benutzt, dann bedeutet das, dass der HERSTELLER diesen PROZESS, diese AKTIVITÄT, diese AUFGABE oder dieses Ergebnis benutzen muss, es sei denn, der HERSTELLER kann eine Rechtfertigung dafür dokumentieren, warum er dies unterlässt.

Einleitung zu Änderung 1

Die erste Ausgabe wurde 2006 veröffentlicht. Diese Ergänzung dient dazu, Anforderungen an ÄLTERE SOFTWARE festzulegen, deren Softwaredesign vor der Veröffentlichung der aktuellen Ausgabe entwickelt wurde, um Hersteller bei der Übereinstimmung dieser Norm mit den europäischen Direktiven zu unterstützen. Die Software-Sicherheitsklassifizierung musste für diese Ergänzung geändert werden einschließlich der Klärung von Anforderungen und Anpassung der Software-Sicherheitsklassifikation, um einen risikobasierten Ansatz einzuführen. Die Arbeit wird für die zweite Ausgabe der IEC 62304 parallel fortgesetzt.

1 Anwendungsbereich

1.1 *Zweck

Diese Norm definiert Anforderungen an den Lebenszyklus von MEDIZINPRODUKTE-SOFTWARE. Die Zusammenstellung von PROZESSEN, AKTIVITÄTEN und AUFGABEN, die in dieser Norm beschrieben werden, legt einen allgemeinen Rahmen für Lebenszyklus-PROZESSE von MEDIZINPRODUKTE-SOFTWARE fest.

1.2 *Anwendungsgebiet

Diese Norm gilt für die Entwicklung und Wartung von MEDIZINPRODUKTE-SOFTWARE, wenn die Software selbst ein MEDIZINPRODUKT ist oder wenn die Software ein eingebetteter oder integraler Bestandteil des fertigen MEDIZINPRODUKTS ist.

ANMERKUNG 1 Diese Norm kann benutzt werden für die Entwicklung und Wartung von Software, die ein eigenständiges Medizinprodukt ist. Zusätzliche Entwicklungsaktivitäten sind aber auf der Systemebene erforderlich, bevor diese Art von Software in Betrieb gehen kann. Diese Systemaktivitäten werden nicht durch diese Norm abgedeckt, sie finden sich in IEC 82304-1¹⁾ [22].

Diese Norm beschreibt PROZESSE, die bestimmt sind für die Anwendung auf Software, die auf einem Prozessor ausgeführt wird, oder die durch andere Software ausgeführt wird (z. B. ein Interpreter), die auf einem Prozessor ausgeführt wird.

Diese Norm gilt unabhängig vom dauerhaften Speichermedium, das für die Speicherung der Software benutzt wird (z. B. Festplatte, optische Platte, permanentes oder „flash memory“).

Diese Norm gilt unabhängig von der Methode, mit der die Software geliefert wird (z. B. Übertragung über ein Netzwerk oder mit E-mail, optische Platte, „flash memory“ oder EEPROM). Die Methode der Software-Lieferung wird selbst nicht als MEDIZINPRODUKTE-SOFTWARE betrachtet.

Diese Norm deckt nicht Validierung und abschließende FREIGABE des MEDIZINPRODUKTS ab, auch dann nicht, wenn das MEDIZINPRODUKT gänzlich aus Software besteht.

ANMERKUNG 2 Wenn ein Medizingerät „embedded software“ enthält, die auf einem Prozessor ausgeführt werden soll, dann gelten die Anforderungen dieser Norm für die Software, einschließlich der Anforderungen für Software unbekannter Herkunft (siehe 8.1.2).

ANMERKUNG 3 Validierung und andere Entwicklungsaktivitäten sind auf der Systemebene erforderlich, bevor die Software und das Medizinprodukt in Betrieb gehen kann. Diese Systemaktivitäten werden nicht durch diese Norm abgedeckt, sie finden sich in den entsprechenden Produktnormen (z. B. IEC 60601-1, IEC 82304-1, etc.).

1.3 Beziehung zu anderen Normen

Diese MEDIZINPRODUKTE-SOFTWARE-Lebenszyklus-Norm soll zusammen mit anderen geeigneten Normen benutzt werden, wenn ein MEDIZINPRODUKT entwickelt wird. [Anhang C](#) stellt die Beziehung zwischen dieser Norm und anderen relevanten Normen her.

1.4 Einhaltung

Die Einhaltung dieser Norm gilt als erfüllt, wenn alle PROZESSE, AKTIVITÄTEN und AUFGABEN, die in dieser Norm im Bezug auf die Software-Sicherheitsklasse festgelegt sind, implementiert wurden.

¹⁾ In Vorbereitung.

ANMERKUNG 1 Jeder Anforderung sind Software-Sicherheitsklassen zugeordnet. Die Angabe der Software-Sicherheitsklassen steht im normativen Text hinter der entsprechenden Anforderung.

Die Einhaltung wird durch das Besichtigen der gesamten Dokumentation festgestellt, die von dieser Norm gefordert wird, einschließlich der RISIKOMANAGEMENT-AKTE, und durch die Beurteilung der PROZESSE, AKTIVITÄTEN und AUFGABEN, die für die entsprechende Software-Sicherheitsklasse gefordert werden.

ANMERKUNG 2 Diese Beurteilung kann durch ein internes oder externes Audit durchgeführt werden.

ANMERKUNG 3 Bei der Ausführung der festgelegten PROZESSE, AKTIVITÄTEN und AUFGABEN bestehen Freiheitsgrade in der Auswahl der Methoden zur Implementierung dieser PROZESSE und der Ausführung dieser AKTIVITÄTEN und AUFGABEN.

ANMERKUNG 4 Für diese Beurteilung ist an den Stellen, an denen bestimmte Anforderungen den Zusatz „soweit angemessen“ enthalten und nicht erfüllt werden, eine Begründung zu dokumentieren.

ANMERKUNG 5 An den Stellen, an denen die ISO/IEC 12207 den Begriff „Übereinstimmung“ verwendet, wird in dieser Norm der Begriff „Einhaltung“ verwendet.

ANMERKUNG 6 Für die Einhaltung von ÄLTERER SOFTWARE siehe 4.4.

2 *Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 14971, *Medical devices – Application of risk management to medical devices*

3 *Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

AKTIVITÄT

Satz von einer oder mehreren aufeinander bezogenen oder sich gegenseitig beeinflussenden AUFGABEN

3.2

ANOMALIE

jeglicher Zustand, der abweicht von dem, was auf Grund von Anforderungsspezifikationen, Entwicklungsdokumenten, Normen usw. oder von Wahrnehmungen oder Erfahrungen zu erwarten ist. ANOMALIEN können sich unter anderem beim Review, bei der Prüfung, der Analyse, der Kompilierung oder bei der Benutzung von MEDIZINPRODUKTE-SOFTWARE oder zugehöriger Dokumentation finden.

Anmerkung 1 zum Begriff: Basierend auf IEEE 1044:1993, 3.1 [18]^{N1)}.

3.3

ARCHITEKTUR

Organisationsstruktur eines SYSTEMS oder einer Komponente

[QUELLE: IEEE 610.12:1990] [17]

^{N1)} Nationale Fußnote: Der Verweis zu den Literaturhinweisen fehlt in der Internationalen Norm.

3.4

ÄNDERUNGSANFORDERUNG

dokumentierte Spezifikation einer Änderung, die an einer MEDIZINPRODUKTE-SOFTWARE durchgeführt werden soll

3.5

KONFIGURATIONSELEMENT

Einheit, die an einem gegebenen Referenzpunkt eindeutig identifiziert werden kann

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 12207:2008, 4.7 [9]

3.6

ZU LIEFERNDEN ERGEBNIS

gefordertes Resultat oder Ergebnis (einschließlich Dokumentation) einer AKTIVITÄT oder AUFGABE

3.7

EVALUATION

systematische Bewertung oder Beurteilung, inwieweit eine Einheit ihre festgelegten Merkmale erfüllt

[QUELLE: ISO/IEC 12207:2008, 4.12] [9]

3.8

SCHADEN

physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt

[QUELLE: ISO 14971:2007, 2.2]

3.9

GEFÄHRDUNG

potenzielle SCHADENS-Quelle

[QUELLE: ISO 14971:2007, 2.3]

3.10

HERSTELLER

natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung oder Kennzeichnung eines MEDIZINPRODUKTS, für den Zusammenbau eines SYSTEMS oder für die Anpassung eines MEDIZINPRODUKTS vor dem Inverkehrbringen oder der Inbetriebnahme verantwortlich ist, unabhängig davon, ob diese Tätigkeiten von dieser Person selbst oder stellvertretend für diese von einer dritten Person ausgeführt werden

Anmerkung 1 zum Begriff: Aufmerksamkeit wird auf die Tatsache gelenkt, dass die Bestimmungen nationaler oder regionaler Vorschriften für die Definition „Hersteller“ gelten können.

Anmerkung 2 zum Begriff: Für eine Definition von „Kennzeichnung“ siehe ISO 13485:2003, Definition 3.6.

[QUELLE: ISO 14971:2007, 2.8]

3.11

MEDIZINPRODUKT

alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Stoffe oder anderen Gegenstände, einschließlich der für ein einwandfreies Funktionieren des MEDIZINPRODUKTS eingesetzten Software, die vom HERSTELLER zur Anwendung für Menschen für folgende Zwecke bestimmt sind:

- Erkennung, Verhütung, Erfassen, Behandlung oder Linderung von Krankheiten,
- Erkennung, Erfassung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,

- Untersuchung, Ersatz oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs,
- Lebenserhaltung oder Lebensunterstützung,
- Empfängnisregelung,
- Desinfektion von MEDIZINPRODUKTEN,
- Bereitstellung von Informationen für medizinische Zwecke mittels In-vitro-Untersuchung von Probestücken des menschlichen Körpers,

und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische noch durch immunologische oder metabolische Mittel erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann

Anmerkung 1 zum Begriff: Diese Definition wurde durch die Global Harmonization Task Force (GHTF) entwickelt. Siehe Literaturhinweis [15] in ISO 13485:2003.

[QUELLE: ISO 13485:2003, Begriff 3.7] [8]

Anmerkung 2 zum Begriff: In den Definitionen, wie sie in den nationalen Regularien des jeweiligen Landes verwendet werden, können Unterschiede auftreten.

Anmerkung 3 zum Begriff: In Verbindung mit IEC 60601-1:2005 und IEC 60601-1:2005/AMD1:2012 hat der Begriff „Medizinprodukt“ die gleiche Bedeutung wie ME-GERÄT oder ME-SYSTEM (dies sind definierte Begriffe nach IEC 60601-1).

3.12

MEDIZINPRODUKTE-SOFTWARE

SOFTWARE-SYSTEM, das entwickelt wurde, um in das in der Entwicklung befindliche MEDIZINPRODUKT integriert zu werden, oder das für die Benutzung als selbständiges MEDIZINPRODUKT vorgesehen ist

Anmerkung 1 zum Begriff: Dies schließt ein MEDIZINPRODUKTE-Software-Produkt ein, was dann ein eigenständiges MEDIZINPRODUKT ist.

3.13

PROBLEMBERICHT

Aufzeichnung über ein tatsächliches oder mögliches Verhalten einer MEDIZINPRODUKTE-SOFTWARE, von dem ein Anwender oder eine andere beteiligte Person glaubt, dass es unsicher, ungeeignet für den bestimmungsgemäßen Gebrauch oder widersprüchlich zur Spezifikation sei

Anmerkung 1 zum Begriff: Diese Norm fordert nicht, dass jeder PROBLEMBERICHT zu einer Änderung der MEDIZINPRODUKTE-SOFTWARE führt. Ein HERSTELLER kann einen PROBLEMBERICHT als Missverständnis, als Fehler oder als unbedeutendes Ereignis ablehnen.

Anmerkung 2 zum Begriff: Ein PROBLEMBERICHT kann sich auf eine freigegebene MEDIZINPRODUKTE-SOFTWARE oder auf eine noch in der Entwicklung befindliche MEDIZINPRODUKTE-SOFTWARE beziehen.

Anmerkung 3 zum Begriff: Diese Norm fordert vom HERSTELLER, dass er für einen PROBLEMBERICHT, der sich auf ein freigegebenes Produkt bezieht, besondere Entscheidungen trifft (siehe Abschnitt 6), um zu gewährleisten, dass regulatorische Maßnahmen identifiziert und implementiert werden.

3.14

Prozess

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Aktivitäten, der Eingaben in Ergebnisse umwandelt

[QUELLE: ISO 9000:2000, Begriff 3.4.1] [6]

ANMERKUNG 1 zum Begriff: Der Begriff „AKTIVITÄTEN“ beinhaltet den Gebrauch von Ressourcen.

3.15

REGRESSIONSPRÜFUNG

Prüfung, die erforderlich ist, um festzustellen, dass eine Änderung einer SYSTEM-Komponente deren Funktionalität, Zuverlässigkeit und Leistungsfähigkeit nicht beeinträchtigt und keine zusätzlichen Defekte verursacht hat

[QUELLE: ISO/IEC 90003:2004, Begriff 3.11] [15]

3.16

RISIKO

Kombination der Wahrscheinlichkeit des Auftretens eines SCHADENS und des Schweregrades dieses SCHADENS

[QUELLE: ISO 14971:2007, 2.16]

3.17

RISIKOANALYSE

systematische Verwendung von verfügbarer Informationen zur Identifizierung von GEFÄHRDUNGEN und Einschätzung von RISIKEN

[QUELLE: ISO 14971:2007, 2.17]

3.18

RISIKOBEHERRSCHUNG

PROZESS, in dem Entscheidungen getroffen und Maßnahmen implementiert werden, durch die RISIKEN auf festgelegte Bereiche verringert oder auf diesen gehalten werden

[QUELLE: ISO 14971:2007, 2.19]^{N2)}

3.19

RISIKOMANAGEMENT

systematische Anwendung von Managementstrategien, Verfahren und Praktiken auf die Aufgaben der Analyse, Bewertung und Beherrschung von RISIKEN

[QUELLE: ISO 14971:2007, 2.22, modifiziert – Der Teil „Überwachung“ wurde entfernt]

3.20

RISIKOMANAGEMENT-ÄKTE

Zusammenstellung von Aufzeichnungen und sonstigen Dokumenten, die durch den RISIKOMANAGEMENT-PROZESS entstehen und nicht notwendigerweise an einer Stelle sein müssen

[QUELLE: ISO 14971:2007, 2.23]

3.21

SICHERHEIT

Freiheit von unvermeidbaren RISIKEN

[QUELLE: ISO 14971:2007, 2.24]

3.22

DATENSICHERHEIT

Schutz von Informationen und Daten derart, dass nicht autorisierte Personen oder Systeme sie nicht lesen oder verändern können und dass autorisierten Personen und Systemen der Zugang zu ihnen nicht verweigert wird

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 12207:2008, 4.39 [9].

^{N2)} Nationale Fußnote: Der Begriff wurde zur besseren Verständlichkeit von „Risikokontrolle“ in „Risikobeherrschung“ geändert. In der Ausgabe DIN EN ISO 14971:2006 wird dieser Begriff ebenfalls verwendet.

3.23

SCHWERE VERLETZUNG

Verletzung oder Krankheit, die

- a) lebensbedrohend ist,
- b) zu einer andauernden Beeinträchtigung einer Körperfunktion oder zu einer andauernden Schädigung des (menschlichen) Körpers führt oder
- c) ein medizinisches oder chirurgisches Eingreifen erfordert, um eine andauernde Beeinträchtigung einer Körperfunktion oder eine andauernde Schädigung des (menschlichen) Körpers zu verhindern

Anmerkung 1 zum Begriff: Andauernde Beeinträchtigung bedeutet eine unumkehrbare Beeinträchtigung oder Schädigung des (menschlichen) Körpers oder einer Körperfunktion und schließt geringfügige Beeinträchtigungen oder Schädigungen aus.

3.24

LEBENSZYKLUS-MODELL DER SOFTWARE-ENTWICKLUNG

konzeptionelle Struktur, welche die Lebenszeit der Software von der Anforderungsdefinition bis zur FREIGABE umfasst und die

- die PROZESSE, AKTIVITÄTEN und AUFGABEN festlegt, die an der Entwicklung einer MEDIZINPRODUKTE-SOFTWARE beteiligt sind,
- die Reihenfolge und die Abhängigkeit von AKTIVITÄTEN und AUFGABEN beschreibt und
- die Meilensteine festlegt, bei denen die Vollständigkeit der festgelegten ZU LIEFERNDEN ERGEBNISSE verifiziert wird

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 12207:1995, 3.11.

3.25

SOFTWARE-KOMPONENTE

jedes identifizierbare Teil eines Computerprogramms, d. h. Quellcode, Objektcode, Kontrollcode Kontroll-daten oder eine Zusammenstellung dieser Teile

Anmerkung 1 zum Begriff: Drei Begriffe kennzeichnen die Zerlegung der Software in einzelne Bestandteile. Die oberste Ebene bildet das SOFTWARE-SYSTEM. Die unterste Ebene, die nicht weiter zerlegt wird, ist die SOFTWARE-EINHEIT. Alle Ebenen, die Bestandteile vereinen, einschließlich der obersten und der untersten Ebene, können als SOFTWARE-KOMPONENTEN bezeichnet werden. Ein SOFTWARE-SYSTEM ist folglich zusammengesetzt aus einer oder mehreren SOFTWARE-KOMPONENTEN, und jede SOFTWARE-KOMPONENTE ist zusammengesetzt aus einer oder mehreren SOFTWARE-EINHEITEN oder zerlegbaren SOFTWARE-KOMPONENTEN. Es ist der Verantwortung des HERSTELLERS überlassen, den Unterteilungsgrad der SOFTWARE-KOMPONENTEN und SOFTWARE-EINHEITEN festzulegen.

Anmerkung 2 zum Begriff: Basierend auf ISO/IEC 90003:2004, 3.14 [15], und ISO/IEC 12207:2008, 4.41 [9].

3.26

Nicht benutzt

3.27

SOFTWARE-SYSTEM

integrierte Sammlung von SOFTWARE-KOMPONENTEN, die so organisiert sind, dass eine spezifische Funktion oder ein Satz von Funktionen ausgeführt werden kann

3.28

SOFTWARE-EINHEIT

SOFTWARE-KOMPONENTE, die nicht in weitere Komponenten unterteilt ist

Anmerkung 1 zum Begriff: Der Unterteilungsgrad von SOFTWARE-EINHEITEN wird vom HERSTELLER definiert (siehe B.3).

3.29

SOFTWARE UNBEKANNTER HERKUNFT (en: SOFTWARE OF UNKNOWN PROVENANCE)

SOUP

SOFTWARE-KOMPONENTE, die bereits entwickelt und allgemein verfügbar ist und die nicht entwickelt wurde, um in das MEDIZINPRODUKT integriert zu werden (auch bekannt als „Off-The-Shelf-Software“), oder zuvor entwickelte SOFTWARE-KOMPONENTE, für die angemessene Aufzeichnungen zum Entwicklungs-PROZESS nicht verfügbar sind

Anmerkung 1 zum Begriff: Ein MEDIZINPRODUKTE-SOFTWARESYSTEM selbst kann nicht beanspruchen, SOFTWARE UNBEKANNTER HERKUNFT (SOUP) zu sein.

3.30

SYSTEM

integrierter Verbund, bestehend aus einem oder mehreren PROZESSEN, Hardware, Software, Einrichtungen und Personen, der eine Fähigkeit zur Verfügung stellt, um einen bestimmten Zweck oder ein bestimmtes Ziel zu erreichen

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 12207:2008, 4.48 [9].

3.31

AUFGABE

eine Teilarbeit, die erledigt werden muss

3.32

RÜCKVERFOLGBARKEIT

Grad in welchem, eine Beziehung zwischen zwei oder mehr Produkten des Entwicklungs-PROZESSES hergestellt werden kann

Anmerkung 1 zum Begriff: Anforderungen, Architektur, RISIKOBEHERRSCHUNGS-Maßnahme etc. sind Beispiele für Ergebnisse des Entwicklungs-PROZESSES.

[QUELLE: IEEE 610.12:1990] [17]

3.33

VERIFIZIERUNG

Bestätigung durch Bereitstellen eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Die Benennung „verifiziert“ wird zur Bezeichnung des entsprechenden Status verwendet.

[QUELLE: ISO 9000:2000, Definition 3.8.4]

Anmerkung 2 zum Begriff: Bei Design und Entwicklung beschäftigt sich die VERIFIZIERUNG mit dem PROZESS der EVALUATION des Ergebnisses einer gegebenen AKTIVITÄT, um festzustellen, dass die für diese AKTIVITÄT aufgestellten Anforderungen eingehalten wurden.

3.34

VERSION

gekennzeichnete Ausgabe eines KONFIGURATIONSELEMENTES

Anmerkung 1 zum Begriff: Die Änderung einer VERSION einer MEDIZINPRODUKTE-SOFTWARE, die in einer neuen VERSION resultiert, erfordert eine Konfigurations-Management-Aktion.

Anmerkung 2 zum Begriff: Basierend auf ISO/IEC 12207:2008, 4.56 [9].

3.35

GEFÄHRDUNGSSITUATION

Umstände, unter denen Menschen, Güter oder die Umwelt einer oder mehreren GEFÄHRDUNGEN ausgesetzt sind

[QUELLE: ISO 14971:2007, 2.4]

3.36

ÄLTERE SOFTWARE

MEDIZINPRODUKTE-SOFTWARE, die legal auf den Markt gebracht wurde und noch heute vermarktet wird, für die jedoch kein ausreichender Nachweis vorhanden ist, dass sie unter Einhaltung der aktuellen Version dieser Norm entwickelt wurde

3.37

FREIGABE

bestimmte VERSION eines KONFIGURATIONSELEMENTES, das für einen spezifischen Zweck verfügbar gemacht wird

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 12207:2008, 4.35 [9].

3.38

RESTRISIKO

RISIKO, das nach Durchführung von Maßnahmen zur RISIKOBEHERRSCHUNG verbleibt

Risiko, das nach der Durchführung von Maßnahmen zur Risikobeherrschung verbleibt

Anmerkung 1 zum Begriff: In Anlehnung an ISO/IEC Guide 51:1999, 3.9 [16].

Anmerkung 2 zum Begriff: ISO/IEC Guide 51:1999, 3.9 [16] verwendet den Begriff „Schutzmaßnahmen“ anstelle „RISIKOBEHERRSCHUNGS-Maßnahmen“. Im Zusammenhang dieser Internationalen Norm sind „Schutzmaßnahmen“ nur eine Wahlmöglichkeit für die RISIKOBEHERRSCHUNG, wie in [ISO 14971:2007, 6.2] beschrieben.

[QUELLE: ISO 14971:2007, 2.15]

3.39

RISIKOEINSCHÄTZUNG

PROZESS, in dem Werte für die Wahrscheinlichkeit des Auftretens eines SCHADENS und dem Schweregrad dieses SCHADENS zugeordnet werden

[QUELLE: ISO 14971:2007, 2.20]

3.40

RISIKOBEURTEILUNG

PROZESS des Vergleichs des eingeschätzten RISIKO mit gegebenen RISIKO-Kriterien, um die Akzeptanz des RISIKOS zu bestimmen

[QUELLE: ISO 14971:2007, 2.21]

4 *Allgemeine Anforderungen

4.1 *Qualitätsmanagement-System

Der HERSTELLER von MEDIZINPRODUKTE-SOFTWARE muss seine Fähigkeit, MEDIZINPRODUKTE-SOFTWARE zu erstellen, die Kundenanforderungen und anwendbare regulatorische Anforderungen dauerhaft erfüllt, nachweisen.

ANMERKUNG 1 Diese Fähigkeit kann durch die Anwendung eines Qualitätsmanagementsystems nachgewiesen werden, das

- ISO 13485 [8] oder

- einer nationalen Norm für Qualitätsmanagement-SYSTEME oder
- einem Qualitätsmanagement-System, das durch nationale Vorschriften gefordert wird, entspricht.

ANMERKUNG 2 Anleitung für die Anwendung von Anforderungen für Qualitätsmanagement-Systeme findet sich in ISO/IEC 90003 [15].

4.2 *RISIKOMANAGEMENT

Der HERSTELLER muss einen RISIKOMANAGEMENT-PROZESS nach ISO 14971 anwenden.

4.3 *Software-Sicherheitsklassifizierung

- a) Der HERSTELLER muss jedem SOFTWARE-SYSTEM eine Software-Sicherheitsklasse (A, B oder C) zuordnen, je nach dem RISIKO eines SCHADENS für den Patienten, den Anwender oder andere Personen, das aus einer GEFÄHRDUNGSSITUATION resultiert, zu der das SOFTWARE-SYSTEM in einem Worst-case-Szenario beitragen kann, wie in Bild 3 gezeigt.

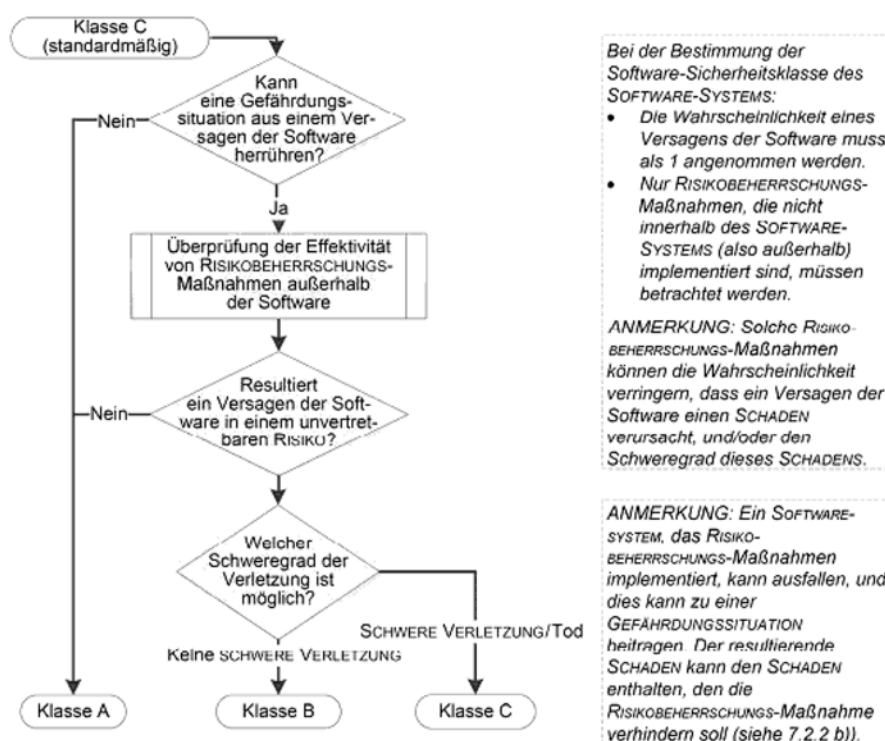


Bild 3 – Zuordnen einer Software-Sicherheitsklasse

Das SOFTWARE-SYSTEM ist Software der Klasse A, wenn:

- das SOFTWARE-SYSTEM nicht zu einer GEFÄHRDUNGSSITUATION beitragen kann oder
- das SOFTWARE-SYSTEM zu einer GEFÄHRDUNGSSITUATION beitragen kann, die nach Betrachtung von RISIKOBEHERRSCHUNGS-Maßnahmen außerhalb des SOFTWARE-SYSTEMS nicht zu einem unvertretbaren RISIKO führen kann.

Das SOFTWARE-SYSTEM ist Software der Klasse B, wenn:

- das SOFTWARE-SYSTEM zu einer GEFÄHRDUNGSSITUATION beitragen kann, die nach Betrachtung von RISIKOBEHERRSCHUNGS-Maßnahmen außerhalb des SOFTWARE-SYSTEMS, zu einem unvertretbaren RISIKO führt, und wenn der resultierende mögliche SCHADEN keine SCHWERE VERLETZUNG ist.

Das SOFTWARE-SYSTEM ist Software der Klasse C, wenn:

- das SOFTWARE-SYSTEM zu einer GEFÄHRDUNGSSITUATION beitragen kann, die nach Betrachtung von RISIKOBEHERRSCHUNGS-Maßnahmen außerhalb des SOFTWARE-SYSTEMS zu einem unvertretbaren RISIKO führt, und wenn der resultierende mögliche SCHADEN Tod oder eine SCHWERE VERLETZUNG ist.

Bei einem Software-System, das ursprünglich als Klasse B oder C eingestuft wurde, kann der Hersteller zusätzliche RISIKOBEHERRSCHUNGS-Maßnahmen außerhalb des Software-Systems implementieren (einschließlich der Überarbeitung der Systemarchitektur, die das Software-System enthält), und er kann danach dem Software-System eine neue Software Klasse zuordnen.

ANMERKUNG 1 Externe RISIKOBEHERRSCHUNGS-Maßnahmen können sein: Hardware, ein unabhängiges SOFTWARE-SYSTEM, Pflegeverfahren oder andere Mittel, um zu minimieren, dass Software zu einer GEFÄHRDUNGSSITUATION beitragen kann.

ANMERKUNG 2: Siehe ISO 14971:2007, 3.2, *Management-Verantwortlichkeiten*, für die Definition von Vertretbarkeit von Risiken.

b) Nicht benutzt.

c) Der HERSTELLER muss die Software-Sicherheitsklasse, die jedem SOFTWARE-SYSTEM zugeordnet wurde, in der RISIKOMANAGEMENT-AKTE dokumentieren.

d) Wenn ein SOFTWARE-SYSTEM in SOFTWARE-KOMPONENTEN zerlegt wird und wenn eine SOFTWARE-KOMPONENTE in weitere SOFTWARE-KOMPONENTEN zerlegt wird, so müssen diese SOFTWARE-KOMPONENTEN die Software-Sicherheitsklasse der ursprünglichen SOFTWARE-KOMPONENTE (oder des SOFTWARE-SYSTEMS) übernehmen, es sei denn, der HERSTELLER dokumentiert eine Begründung für die Klassifizierung in eine andere Software-Sicherheitsklasse (Zuordnung der Software Sicherheitsklassen nach 4.3 a). Eine solche Begründung muss darlegen, wie die neuen SOFTWARE-KOMPONENTEN so abgegrenzt sind, dass sie getrennt klassifiziert werden können.

e) Der HERSTELLER muss die Software-Sicherheitsklasse jeder SOFTWARE-KOMPONENTE dokumentieren, wenn sich deren Klasse von der Klasse derjenigen SOFTWARE-KOMPONENTE, aus der sie durch Zerlegung entstanden ist, unterscheidet.

f) Wenn diese Norm auf eine Gruppe von SOFTWARE-KOMPONENTEN angewandt wird, muss der HERSTELLER, um diese Norm einzuhalten, diejenigen PROZESSE und AUFGABEN verwenden, die durch die Klassifizierung der am höchsten klassifizierten SOFTWARE-KOMPONENTE in dieser Gruppe gefordert werden, es sei denn, der HERSTELLER dokumentiert eine Begründung für die Verwendung einer niedrigeren Klasse in der RISIKOMANAGEMENT-AKTE.

g) Bis eine Software-Sicherheitsklasse zugeordnet ist, gelten für jedes SOFTWARE-SYSTEM die Anforderungen der Klasse C.

ANMERKUNG Bei den folgenden Abschnitten und Unterabschnitten werden die Software-Sicherheitsklassen, für die bestimmte Anforderungen gelten, in der Form [Klasse ...] nach der Anforderung festgelegt.

4.4 *ÄLTERE SOFTWARE

4.4.1 Allgemeines

Als eine Alternative zur Anwendung der Abschnitte 5 bis 9 dieser Norm kann für ÄLTERE SOFTWARE die Einhaltung gezeigt werden, wie in 4.4.2 bis 4.4.5 beschrieben.

4.4.2 RISIKOMANAGEMENT-AKTIVITÄTEN

In Übereinstimmung mit 4.2 dieser Norm muss der HERSTELLER:

- a) alle Rückmeldungen über ÄLTERE SOFTWARE, einschließlich Informationen aus der Nach-Produktionsphase, hinsichtlich Unfällen oder Beinahe-Unfällen untersuchen, und zwar sowohl aus seiner eigenen Organisation als auch von Benutzern;
- b) RISIKOMANAGEMENT-AKTIVITÄTEN durchführen im Zusammenhang mit der weiteren Verwendung der ÄLTEREN SOFTWARE, unter Berücksichtigung folgender Aspekte:
 - Integration der ÄLTEREN SOFTWARE in die Gesamtarchitektur des MEDIZINPRODUKTES;
 - weitere Gültigkeit von RISIKOBEHERRSCHUNGS-Maßnahmen, die als Teil der ÄLTEREN SOFTWARE implementiert wurden;
 - Identifizierung von GEFÄHRDUNGSSITUATIONEN im Zusammenhang mit der weiteren Verwendung der ÄLTEREN SOFTWARE;
 - Identifizierung möglicher Ursachen für den Beitrag der ÄLTEREN SOFTWARE zu einer GEFÄHRDUNGSSITUATION;
 - Definition von RISIKOBEHERRSCHUNGS-Maßnahmen für jede mögliche Ursache eines Beitrags der ÄLTEREN SOFTWARE zu einer GEFÄHRDUNGSSITUATION;

4.4.3 Lückenanalyse

Basierend auf der Software Sicherheitsklasse der ÄLTEREN SOFTWARE (siehe 4.3) muss der HERSTELLER eine Lückenanalyse der verfügbaren ZU LIEFERNDEN ERGEBNISSE gegenüber denen, die in 5.2, 5.3, 5.7 und Abschnitt 7 gefordert werden, durchführen.

- a) Der HERSTELLER muss die weitere Gültigkeit der verfügbaren ZU LIEFERNDEN ERGEBNISSE bewerten.
- b) Soweit Lücken identifiziert werden, muss der HERSTELLER die mögliche Reduzierung des RISIKOS beurteilen, die aus der Erzeugung der fehlenden ZU LIEFERNDEN ERGEBNISSE und der damit zusammenhängenden AKTIVITÄTEN resultiert.
- c) Basierend auf dieser Beurteilung muss der HERSTELLER bestimmen, welche ZU LIEFERNDEN ERGEBNISSE erzeugt werden und welche der damit zusammenhängenden AKTIVITÄTEN durchgeführt werden müssen. Das minimale ZU LIEFERNDE ERGEBNIS müssen Aufzeichnungen der SOFTWARE-SYSTEM Prüfungen sein (siehe 5.7.5).

ANMERKUNG Diese Lückenanalyse soll sicherstellen, dass RISIKOBEHERRSCHUNGS-Maßnahmen, die in die ÄLTERE SOFTWARE implementiert wurden, in den Software Anforderungen enthalten sind.

4.4.4 Aktivitäten für das Schließen der Lücken

- a) Der HERSTELLER muss einen Plan für die Erzeugung der identifizierten ZU LIEFERNDEN ERGEBNISSE festlegen und durchführen. Soweit verfügbar kann ein objektiver Nachweis zur Erzeugung der geforderten ZU LIEFERNDEN ERGEBNISSE benutzt werden, ohne Durchführung der AKTIVITÄTEN, die in 5.2, 5.3, 5.7 und Abschnitt 7 gefordert sind.

ANMERKUNG Ein Plan, wie die identifizierten Lücken bearbeitet werden, kann in einem Software-Wartungsplan enthalten sein (siehe 6.1)

- b) Der Plan muss die Benutzung des Problemlösungs-PROZESSES für die Bearbeitung von Problemen, die in der ÄLTEREN SOFTWARE und in den ZU LIEFERNDEN ERGEBNISSEN entdeckt wurden, in Übereinstimmung mit Abschnitt 9 adressieren.
- c) Änderungen an der ÄLTEREN SOFTWARE müssen in Übereinstimmung mit Abschnitt 6 durchgeführt werden.

4.4.5 Begründung für die Benutzung der ÄLTEREN SOFTWARE

Der HERSTELLER muss die VERSION der ÄLTEREN SOFTWARE dokumentieren, zusammen mit einer Begründung für die weitere Benutzung der ÄLTEREN SOFTWARE, basierend auf den Ergebnissen von 4.4.

ANMERKUNG Das Einhalten von 4.4 ermöglicht die weitere Benutzung der ÄLTEREN SOFTWARE in Übereinstimmung mit IEC 62304

5 *Software-Entwicklungs-PROZESS

5.1 *Planung der Software-Entwicklung

5.1.1 Software-Entwicklungsplan

Der HERSTELLER muss einen Software-Entwicklungsplan (oder -pläne) für die Durchführung der AKTIVITÄTEN des Software-Entwicklungs-PROZESSES erstellen. Dieser PROZESS muss dem Anwendungsbereich, dem Umfang und den Software-Sicherheitsklassen des zu entwickelnden SOFTWARE-SYSTEMS angemessen entsprechen. Das LEBENSZYKLUS-MODELL DER SOFTWARE-ENTWICKLUNG muss entweder vollständig definiert oder im Plan (in den Plänen) referenziert sein. Der Plan muss folgende Punkte umfassen:

- a) die PROZESSE, die bei der Entwicklung des SOFTWARE-SYSTEMS verwendet werden (siehe Anmerkung 4);
- b) die ZU LIEFERNDEN ERGEBNISSE (einschließlich der Dokumentation) der AKTIVITÄTEN und AUFGABEN;
- c) RÜCKVERFOLGBARKEIT zwischen SYSTEM-Anforderungen, Software-Anforderungen, SOFTWARE-SYSTEM-Prüfungen und RISIKOKONTROLL-Maßnahmen, die in Software implementiert werden;
- d) Software-Konfigurations- und Änderungsmanagement, einschließlich SOUP-KONFIGURATIONSELEMENTEN und Software, die zur Entwicklungsunterstützung verwendet wird;
- e) Software-Problemlösung und Behandlung von Problemen, die bei MEDIZINPRODUKTE-SOFTWARE, ZU LIEFERNDEN ERGEBNISSEN und AKTIVITÄTEN in jeder Phase des Lebenszyklus entdeckt werden.

[Klasse A, B, C]

ANMERKUNG 1 Das LEBENSZYKLUS-MODELL DER SOFTWARE-ENTWICKLUNG kann unterschiedliche Elemente (PROZESSE, AKTIVITÄTEN, AUFGABEN und ZU LIEFERNDE ERGEBNISSE) für unterschiedliche SOFTWARE-KOMPONENTEN entsprechend der Software-Sicherheitsklassifizierung für jede SOFTWARE-KOMPONENTE des SOFTWARE-SYSTEMS festlegen.

ANMERKUNG 2 Diese AKTIVITÄTEN und AUFGABEN können überlappend sein, können sich gegenseitig beeinflussen und können iterativ oder rekursiv durchgeführt werden. Es ist nicht die Absicht, die Anwendung eines bestimmten Lebenszyklus-Modells vorauszusetzen.

ANMERKUNG 3 Andere PROZESSE werden in dieser Norm getrennt vom Entwicklungs-PROZESS beschrieben. Dies bedeutet nicht, dass sie als getrennte AKTIVITÄTEN und AUFGABEN implementiert werden müssen. Die AKTIVITÄTEN und AUFGABEN der anderen PROZESSE können in den Entwicklungs-PROZESS integriert werden.

ANMERKUNG 4 Der Software-Entwicklungsplan kann auf bestehende PROZESSE verweisen oder neue definieren.

ANMERKUNG 5 Der Software-Entwicklungsplan kann in einen Gesamt-SYSTEM-Entwicklungsplan integriert sein

5.1.2 Aktualisierung des Software-Entwicklungsplans

Soweit angemessen, muss der HERSTELLER den Plan dem Entwicklungsfortschritt entsprechend aktualisieren. [Klasse A, B, C]

5.1.3 Referenz im Software-Entwicklungsplan auf SYSTEM-Design und -Entwicklung

- a) Der HERSTELLER muss SYSTEM-Anforderungen im Software-Entwicklungsplan als Vorgaben für die Software-Entwicklung referenzieren.

- b) Der HERSTELLER muss im Software-Entwicklungsplan Verfahren zur Koordination von Software-Entwicklung und Systementwicklung einschließen oder referenzieren; dies ist für die Erfüllung von 4.1 erforderlich (wie z. B. Systemintegration, VERIFIZIERUNG und Validierung).

[Klasse A, B, C]

ANMERKUNG Es kann möglicherweise keinen Unterschied zwischen SOFTWARE-SYSTEM-Anforderungen und SYSTEM-Anforderungen geben, wenn das SOFTWARE-SYSTEM ein eigenständiges SYSTEM (eigenständiges Softwareprodukt) ist.

5.1.4 Planung von Normen, Methoden und Werkzeugen der Software-Entwicklung

Der HERSTELLER muss im Software-Entwicklungsplan einschließen oder referenzieren:

- a) Normen,
- b) Methoden und
- c) Werkzeuge,

die im Zusammenhang mit der Entwicklung von SOFTWARE-KOMPONENTEN der Klasse C stehen. [Klasse C]

5.1.5 Planung der Software-Integration und der Integrationsprüfung

Der HERSTELLER muss im Software-Entwicklungsplan einen Plan einschließen oder referenzieren, wie die SOFTWARE-KOMPONENTEN (einschließlich SOUP) integriert und wie während der Integration Prüfungen durchgeführt werden. [Klasse B, C]

ANMERKUNG 1 Es ist vertretbar, die Integrationsprüfung und die SOFTWARE-SYSTEM-Prüfung in einem Plan und einem Satz von AKTIVITÄTEN zu kombinieren.

ANMERKUNG 2 Siehe 5.6.

5.1.6 Planung der Software-VERIFIZIERUNG

Der HERSTELLER muss im Software-Entwicklungsplan folgende Informationen über die VERIFIZIERUNG einschließen oder referenzieren:

- a) ZU LIEFERNDE ERGEBNISSE, die eine VERIFIZIERUNG erfordern,
- b) die erforderlichen VERIFIZIERUNGS-AUFGABEN für jede AKTIVITÄT des Lebenszyklus,
- c) Meilensteine, bei denen die ZU LIEFERNDEN ERGEBNISSE VERIFIZIERT werden, und
- d) die Akzeptanzkriterien für die VERIFIZIERUNG der ZU LIEFERNDEN ERGEBNISSE.

[Klasse A, B, C]

5.1.7 Planung des Software-RISIKOMANAGEMENTS

Der HERSTELLER muss im Software-Entwicklungsplan einen Plan einschließen oder referenzieren, wie die AKTIVITÄTEN und AUFGABEN des Software-RISIKOMANAGEMENTS durchgeführt werden, einschließlich des Managements von RISIKEN, die sich auf SOUP beziehen. [Klasse A, B, C]

ANMERKUNG Siehe Abschnitt 7.

5.1.8 Planung der Dokumentation

Der HERSTELLER muss Informationen über die Dokumente, die während des Software-Entwicklungszyklus erzeugt werden sollen, in den Software-Entwicklungsplan mit einschließen oder in diesem referenzieren. Für jedes identifizierte Dokument oder jede Art von Dokumenten müssen die folgenden Informationen enthalten sein oder referenziert werden:

- a) Titel, Benennung/Bezeichnung oder Konvention der Benennung/Bezeichnung;

- b) Zweck;
- c) Verfahren und Verantwortlichkeiten für Entwicklung, Überprüfung, Genehmigung und Änderung.

[Klasse A, B, C]

ANMERKUNG Siehe [Abschnitt 8](#) für Überlegungen zum Konfigurationsmanagement der Dokumentation.

5.1.9 Planung des Software-Konfigurationsmanagements

Der HERSTELLER muss im Software-Entwicklungsplan Informationen über das Software-Konfigurationsmanagement einschließen oder referenzieren. Die Information über das Software-Konfigurationsmanagement muss Folgendes enthalten oder referenzieren:

- a) die Klassen, Arten, Kategorien oder Listen von Komponenten, die kontrolliert werden sollen;
- b) die AKTIVITÄTEN und AUFGABEN des Software-Konfigurationsmanagements;
- c) die Organisation(en), die für die Durchführung der Software-Konfigurationsmanagement-AKTIVITÄTEN verantwortlich ist (sind);
- d) deren Beziehung zu anderen Organisationen, wie zum Beispiel der Software-Entwicklung oder -Wartung;
- e) wann die Komponenten unter Konfigurationskontrolle gestellt werden sollen;
- f) wann der Problemlösungs-PROZESS benutzt werden soll.

[Klasse A, B, C]

ANMERKUNG Siehe [Abschnitt 8](#).

5.1.10 Zu kontrollierende unterstützende Komponenten

Zu den zu kontrollierenden Komponenten gehören Werkzeuge, Elemente oder Einstellungen, die zur Entwicklung der MEDIZINPRODUKTE-SOFTWARE benötigt werden und die die MEDIZINPRODUKTE-SOFTWARE beeinflussen könnten. [Klasse B, C]

ANMERKUNG 1 Beispiele für solche Komponenten sind Compiler-/Assembler-VERSIONEN, Make-Dateien, Batch-Dateien und spezifische Einstellungen der Entwicklungsumgebung.

ANMERKUNG 2 Siehe [Abschnitt 8](#).

5.1.11 Kontrolle der Software-KONFIGURATIONSELEMENTE vor der VERIFIZIERUNG

Der HERSTELLER muss planen, die KONFIGURATIONSELEMENTE unter eine Konfigurationsmanagement-Kontrolle zu stellen, bevor sie VERIFIZIERT werden. [Klasse B, C]

5.1.12 Identifizierung und Vermeidung gemeinsamer Software-Fehler

Der HERSTELLER muss im Software-Entwicklungsplan ein Verfahren für Folgendes einschließen oder referenzieren:

- a) Identifizierung von Kategorien von Fehlern, die auf Grund der gewählten Programmier-Technologie eingeführt werden können und die relevant sind für ihr SOFTWARE-SYSTEM, und
- b) Dokumentation des Nachweises, der zeigt, dass diese Fehler nicht zu einem unvermeidbaren RISIKO beitragen.

ANMERKUNG Siehe IEC/TR 80002-1:2009, Anhang B für Beispiele von Kategorien von Fehlern oder von Ursachen, die zu GEFÄHRDUNGSSITUATIONEN beitragen.

[Klasse B, C]